

# Release Notes

## FortiAuthenticator 6.4.1



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



April 21, 2022

FortiAuthenticator 6.4.1 Release Notes

23-641-763282-20220421

# TABLE OF CONTENTS

<b>Change log</b>	<b>5</b>
<b>FortiAuthenticator 6.4.1 release</b>	<b>6</b>
<b>Special notices</b>	<b>7</b>
TFTP boot firmware upgrade process	7
Monitor settings for GUI access	7
Before any firmware upgrade	7
After any firmware upgrade	7
FortiAuthenticator does not support PEAP-MAB	7
<b>What's new</b>	<b>8</b>
Logging: Support for sending syslog messages through an encrypted tunnel	8
Windows Agent: TOTP offline cache size increased	8
RADIUS service: Import clients through CSV file or REST API	8
FSSO: Support for encrypted syslog sources	8
FortiTokens: Ability to report inactive tokens	9
User Portal: Support for the SmartConnect Android application	9
Support for EAP-MSCHAPv2	9
New SAML IdP and Kerberos SSO toggles	9
Windows Agent: Emergency Offline Access	9
OpenID Connect	10
Secure LDAP: Support multiple CAs	10
Import trusted CA certificates with certificate chain	10
Self-service portal: Email templates for resetting password	10
TACACS+: Stronger client secret values	11
SMTP test window provides more accurate error information	11
RADIUS service: Return user group attributes on AD computer authentication	11
SNMP: TACACS+ OIDs	11
OAuth service: Access token expiry	11
Built-in read-only admin profile	12
Additional system information via REST API	12
Log out a session from the monitor page	12
SAML IdP: Support for multiple remote LDAP custom attributes	12
<b>Upgrade instructions</b>	<b>13</b>
Hardware and VM support	13
Image checksums	13
Upgrading from FortiAuthenticator 4.x/5.x/6.x	14
<b>Product integration and support</b>	<b>17</b>
Web browser support	17
FortiOS support	17
Fortinet agent support	17
Virtualization software support	18
Third-party RADIUS authentication	18

---

<b>FortiAuthenticator-VM .....</b>	<b>19</b>
<b>Resolved issues .....</b>	<b>20</b>
<b>Known issues .....</b>	<b>26</b>
<b>Maximum values for hardware appliances .....</b>	<b>29</b>
<b>Maximum values for VM .....</b>	<b>33</b>

## Change log

Date	Change Description
2021-12-01	Initial release.
2021-12-07	Removed bug 756752 from <a href="#">Resolved issues on page 20</a> .
2021-12-10	Updated <a href="#">Upgrade instructions on page 13</a> .
2021-12-31	Updated <a href="#">Upgrade instructions on page 13</a> .
2022-02-24	Updated <a href="#">Maximum values for VM on page 33</a> .
2022-03-02	Added FortiAuthenticator Agent for Microsoft Windows 4.1 to <a href="#">Product integration and support on page 17</a> .
2022-04-21	Removed bug 744940 from <a href="#">Known issues on page 26</a> .

# FortiAuthenticator 6.4.1 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.4.1, build 0958.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: <https://docs.fortinet.com/product/fortiauthenticator/>

## Special notices

### TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

### Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

### Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. From the administrator dropdown menu in the toolbar, go to **Restore/Backup**, and click **Download Backup File** to backup the configuration.

### After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

### FortiAuthenticator does not support PEAP-MAB

FortiAuthenticator only supports MAB in clear-text and not the encapsulated MAB.

## What's new

FortiAuthenticator version 6.4.1 includes the following enhancement:

### Logging: Support for sending syslog messages through an encrypted tunnel

When creating or editing a syslog server in **Logging > Log Config > Syslog Servers**, there is a new **Secure Connection** pane for sending syslog messages to remote servers using a TLS connection.

### Windows Agent: TOTP offline cache size increased

FortiAuthenticator Agent for Microsoft Windows now allows TOTP cache sizes up to 200 days. See Tokens and the *FortiAuthenticator Agent for Microsoft Windows Install Guide* on [Fortinet Docs Library](#).

### RADIUS service: Import clients through CSV file or REST API

RADIUS clients can be imported and assigned to RADIUS policies through a CSV file.

New `radiusclients`, `radiuspolicies`, and `radiuspolicyclient` endpoints available, see [REST API Solutions Guide](#).

### FSSO: Support for encrypted syslog sources

FortiAuthenticator now supports receiving messages from a syslog source over a TLS connection on the port 6514.

Network interfaces in **System > Network > Interfaces** have a new **Syslog over TLS (TCP/6514)** toggle in **Services** that allows receiving messages from a syslog source over TLS.

The syslog-based FSSO feature allows enabling or disabling encrypted syslogs:

- New **Allow TLS encryption** and **Require client authentication** toggle in **Enable Syslog SSO** when editing SSO configuration in **Fortinet SSO Methods > SSO > General**.

A new **TLS encryption** toggle when creating or editing a syslog source in **Fortinet SSO Methods > SSO > Syslog Sources**.



## FortiTokens: Ability to report inactive tokens

You can now see the last used date and time for a FortiToken when editing a FortiToken in **Authentication > User Management > FortiTokens**.

A new last used column in **Authentication > User Management > FortiTokens**.

New `last_used_at` field is available in the `fortitokens` endpoint. See [REST API Solutions Guide](#).

## User Portal: Support for the SmartConnect Android application

FortiAuthenticator now supports the SmartConnect Android application in the captive and self-service user portals.

Android 11 allows the SmartConnect app to install user credential certificates for EAP-TLS and PEAP to allow for user authentication.



Android 11 restricts the SmartConnect app from installing global CA certificates. As of Android 11, these certificates have to be installed manually. A warning message appears in the SmartConnect app, which prompts to install certificates manually.

---

## Support for EAP-MSCHAPv2

FortiAuthenticator now supports EAP-MSCHAPv2 authentication mechanism against a remote AD server.

FortiAuthenticator also supports multi-factor authentication over EAP-MSCHAPv2.

When creating or editing a RADIUS policy in **Authentication > RADIUS Service > Policies**, a new **EAP-MSCHAPv2** toggle is now available in the **Authentication type** tab, given that **Accept EAP** toggle is enabled in **Password/OTP authentication**.

## New SAML IdP and Kerberos SSO toggles

When editing an interface in **System > Network > Interfaces**, new **SAML IdP** and **Kerberos SSO** toggles available in the **Services** pane.

## Windows Agent: Emergency Offline Access

FortiAuthenticator now supports a new temporary token option that allows the use of emergency codes for offline end-users who find themselves without access to FortiToken, email, or SMS.

A new **Enable emergency codes** toggle and **Emergency codes valid for** option when editing the token policy settings in **Authentication > User Account Policies > Tokens**.

A new **Display emergency code** button that displays the emergency code from within a user account if FortiToken is provisioned for the account.

## OpenID Connect

OpenID Connect (OIDC) provides an identity layer on top of the OAuth 2.0 protocol to verify end-user identity and obtain profile information. OIDC is a modern SSO protocol that is easier and more flexible to use than SAML.

OIDC authentication can be enabled for the OAuth client by configuring the relying party with an authorization code, policy, redirect URI, and OIDC claim(s).

**OAuth Service** in **Authentication** has been reorganized to include the following tabs:

- **General**- Configure general settings for OAuth.
- **Policies** - Create policies to use with OAuth authentication.
- **Relying Party** - Configure OAuth clients and OIDC claims.

New OIDC endpoints are now available. The `token` endpoint now expanded to include new fields that support the OIDC configuration. See [REST API Solutions Guide](#).

## Secure LDAP: Support multiple CAs

When creating or editing an LDAP Server in **Authentication > Remote Auth. Servers > LDAP**, a new **Trusted CA** toggle now allows you to specify multiple trusted CAs for secure connection to a remote LDAP server.

## Import trusted CA certificates with certificate chain

Using the new **Learn Certificate** button in **Certificate Management > Certificate Authorities > Trusted CAs**, you can now extract a certificate chain from a TLS server and show its CA certificates by entering the host name/ IP address and the port number. You can then import CA certificates.

## Self-service portal: Email templates for resetting password

New **Password Reset Email Subject** and **Password Reset Email Message** replacement messages in **Authentication > Portals > Replacement Messages**.

## TACACS+: Stronger client secret values

You can now set stronger TACACS+ client secrets to include special characters: `!@#$%^&()_+<>?. /` when adding, editing, or importing TACACS+ clients.

`tacplusclients` endpoint now allows special characters for the `secret` field. See [REST API Solutions Guide](#).

## SMTP test window provides more accurate error information

Upon a failed SMTP test, FortiAuthenticator displays a message in the GUI to help troubleshoot the source of the issue.

For SMTP servers, FortiAuthenticator logs the source of the issue to **Logging > Log Access > Logs**.

Also, upon a failed SMTP send attempt, i.e., when not using the **Test Connection** button, FortiAuthenticator logs the source of the issue to **Logging > Log Access > Logs**.

## RADIUS service: Return user group attributes on AD computer authentication

In the **RADIUS response** tab, when the **AD Computer Authentication Result** is successful and the user is not authenticated yet, you can now select between the following RADIUS attribute response options:

- When **Return User Group Attributes** is enabled, RADIUS attributes configured in the user groups that the computer is a member of are returned.
- **Return Additional Attributes**.

## SNMP: TACACS+ OIDs

FortiAuthenticator adds support for TACACS+ over SNMP which is equivalent to RADIUS.

When configuring SNMP settings in **System > Administration > SNMP**, there is a new **TACACS+ Authentication Client Table Nearly Full Trap Threshold (%)** field to adjust the TACACS+ SNMP trap threshold.

You can enable or disable TACACS+ NAS trap from within SNMP clients (SNMP v3 and SNMP v1/v2) using the new **TACAS+ NAS threshold exceeded** toggle.

## OAuth service: Access token expiry

FortiAuthenticator now returns the remaining validity time for the OAuth2 access token in the `verify_token` endpoint.

A new `expires_in` field is available in the `verify_token` endpoint. See [REST API Solutions Guide](#).

## Built-in read-only admin profile

A new built-in read-only admin profile in **System > Administration > Admin Profiles**.

## Additional system information via REST API

The following new fields are available in the `systeminfo` endpoint:

- `cpu`
- `disk`
- `disk_usage_detail`
- `firmware`
- `memory`
- `memory_usage_detail`

For information about the new fields, see [REST API Solutions Guide](#).

## Log out a session from the monitor page

FortiAuthenticator now allows manually logging out of IdP sessions using the new **Logoff All** and **Logoff Selected** buttons in **Monitor > Authentication > SAML IdP Session**.

## SAML IdP: Support for multiple remote LDAP custom attributes

FortiAuthenticator now supports multiple values for a remote LDAP custom attribute in **Authentication > SAML IdP > Service Providers**.

# Upgrade instructions



Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the [FortiAuthenticator Administration Guide](#).

---

## Hardware and VM support

FortiAuthenticator 6.4.1 supports:

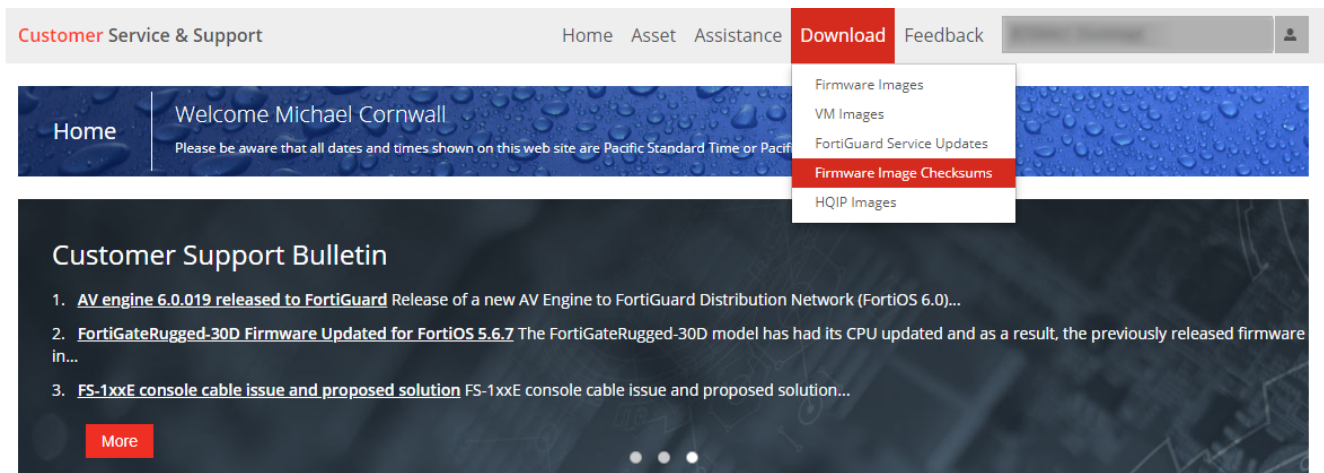
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

## Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the [Fortinet Support](#) website.

## Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

## Upgrading from FortiAuthenticator 4.x/5.x/6.x

FortiAuthenticator 6.4.1 build 0958 officially supports upgrades from previous versions by following these supported FortiAuthenticator upgrade paths:

- If currently running FortiAuthenticator 6.0.5 or older, first upgrade to 6.0.7, then upgrade to 6.4.1, else the following message will be displayed: Image validation failed: The firmware image model number is different from the appliance's.
- If currently running FortiAuthenticator 6.0.7, then upgrade to 6.4.1 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.4.1.
- If currently running FortiAuthenticator between 6.2.1 and 6.3.x, then upgrade to 6.4.1 directly.



When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.4.1 from FortiAuthenticator 6.0.7, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See [Upgrading KVM / Xen virtual machines on page 15](#).



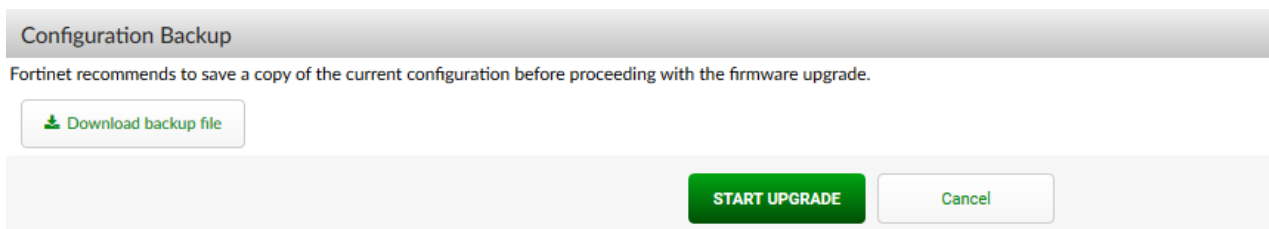
Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

## Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the [Fortinet Support](#) website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the [Fortinet Support](#) website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Upload the firmware and begin the upgrade.  
When upgrading from FortiAuthenticator 6.0.4 and earlier:
  - a. Go to **System > Dashboard > Status**.
  - b. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
  - c. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.When upgrading from FortiAuthenticator 6.1.0 or later:
  - a. Click on the administrator name in the upper-right corner of the GUI to display the dropdown menu, and click **Upgrade**.
  - b. In the **Firmware Upgrade or Downgrade** section, select **Upload a file**, and locate the upgrade package that you downloaded.
5. Select **OK** to upload the file to the FortiAuthenticator.  
Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.  
Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.



Due to a known issue in 6.0.x and earlier releases, the port5 and port6 fiber ports are inverted in the GUI for FAC-3000E models (i.e. port5 in the GUI corresponds to the physical port6 and vice-versa).

This is resolved in 6.1.0 and later, however, the upgrade process does not swap these configurations automatically. If these ports are used in your configuration during the upgrade from 6.0.x to 6.1.0 and later, you will need to physically swap the port5 and port6 fibers to avoid inverting your connections following the upgrade.

## Upgrading KVM / Xen virtual machines

When upgrading existing KVM and Xen virtual machines from FortiAuthenticator 6.0.7 to 6.4.1, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.



If your virtual machine has snapshots, the resize commands detailed below will exit with an error. You must delete the snapshots in order to perform this resize operation. Please make a separate copy of the virtual disk drives before deleting snapshots to ensure you have the ability to rollback.

---

**Use the following command to run the resize on KVM:**

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

**Use the following command to run the resize on Xen:**

```
qemu-img resize /path/to/facxen.qcow2 1G
```

After this command has been completed, you may proceed with the upgrade from 6.0.7 to 6.4.1

## Recovering improperly upgraded KVM / Xen virtual machines

If the upgrade was performed without completing the resize operation above, the virtual machine will fail to properly boot, instead displaying many **initd** error messages. If no snapshots are available, manual recovery is necessary.

To recover your virtual machine, you will need to replace the operating system disk with a good copy, which also requires write-access to the virtual hard disks in the file system while the virtual machines are in an offline state, fully powered down.

**To recover an improperly upgraded KVM virtual machine:**

1. Download the 6.0.7 GA ZIP archive for KVM, **FAC\_VM\_KVM-v6-build0059-FORTINET.out.kvm.zip**.
2. Extract the archive, then replace your virtual machine's **fackvm.qcow2** with the one from the archive.
3. Execute the following command:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

**To recover an improperly upgraded Xen virtual machine:**

1. Download the 6.0.7 GA ZIP archive for Xen, **FAC\_VM\_XEN-v6-build0059-FORTINET.out.xen.zip**.
2. Extract the archive, then replace your virtual machine's **facxen.qcow2** with the one from the archive.
3. Execute the following command:

```
qemu-img resize /path/to/facxen.qcow2 1G
```



# Product integration and support

## Web browser support

The following web browsers are supported by FortiAuthenticator 6.4.1:

- Microsoft Edge version 96
- Mozilla Firefox version 94
- Google Chrome version 95

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS support

FortiAuthenticator 6.4.1 supports the following FortiOS versions:

- FortiOS v7.0.x
- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x

## Fortinet agent support

FortiAuthenticator 6.4.1 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows and macOS (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.6, 3.7, 3.8, 4.0\*, and 4.1\*.
- FortiAuthenticator Agent for Outlook Web Access 2.2
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

\*FortiAuthenticator Agent for Microsoft Windows 4.0 and above required to support emergency offline access. Also, FortiAuthenticator Agent for Microsoft Windows below 4.0 compatible for all other features.

## Virtualization software support

FortiAuthenticator 6.4.1 supports:

- VMware ESXi / ESX 6/7
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- Amazon AWS
- Microsoft Azure
- Oracle OCI
- Alibaba Cloud



Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

---

See [FortiAuthenticator-VM on page 19](#) for more information.

## Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor.
- Token Passcode Appended - Supports any RADIUS compatible system.

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

# FortiAuthenticator-VM

For information about FortiAuthenticator-VM deployments and system requirements, see the VM installation guide on the [Fortinet Docs Library](#).

## Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the [Fortinet Support](#) website.

Bug ID	Description
<b>758522</b>	SP server certificate when expired produces a server 500 when trying to edit the SP configuration.
<b>744936</b>	Yubikey third party token failed authentication with "invalid token" error after FortiAuthenticator upgrades to version 6.4.0.
<b>742360</b>	Remote user sync not reflecting LDAP user's OU change.
<b>758011</b>	Logout from SAML FSSO portal is generating signature validation error and 403 forbidden upon re-authentication.
<b>749761</b>	FortiAuthenticator did not update user group info after sync user from LDAP server.
<b>739254</b>	Uploading CRL on LB secondary FortiAuthenticator causes GUI crash.
<b>754239</b>	LB secondary not syncing when we failover to the secondary FortiAuthenticator.
<b>755884</b>	History password policy not working.
<b>754589</b>	Push Service does not recognize the realm from the FortiAuthenticator agent.
<b>745679</b>	"Mandatory password and OTP" setting not enforcing OTP on unimported remote users.
<b>743480</b>	User sync rule now updates FortiToken assignment if a manual change occurs after initial sync.
<b>751605</b>	Timezone 63 Darwin shows time 1 hour ahead.
<b>753910</b>	Users Audit export: comma separated displayname shifts the cells/fields to the right.
<b>756798</b>	Self-service portal "Change Password" button returns 403 Forbidden error for remote users.
<b>744321</b>	Mobile FortiToken and SMS tokens log event from a scheduled syncing of remote LDAP users.
<b>731626</b>	Limit of 64 characters in SAN DNS field for CSR/Certificate creation.
<b>611922</b>	Improve SCEP grid layout.
<b>735782</b>	Alcatel RADIUS VSA dictionary needs to be updated.
<b>755539</b>	User lookup triggers internal server error 500 for users with two or more IdP sessions.
<b>670317</b>	Not possible to resize/change columns width in log table.
<b>712251</b>	Column resize or sort does not work properly in tables of FortiAuthenticator.
<b>748818</b>	SCEP and device enrollment does not work.
<b>752935</b>	500 internal server error when using unknown email address for password reset.
<b>744768</b>	FortiAuthenticator not logging LDAP group membership changes.
<b>741495</b>	When trying to import users from FortiGate conf to FortiAuthenticator v6.4.

Bug ID	Description
<b>729674</b>	FortiToken license status on LB nodes shows unknown.
<b>748270</b>	IdP proxy scenario with local AD for group membership does not work.
<b>741357</b>	Unable to download raw log.
<b>730640</b>	When signing a CSR via SCEP, FortiAuthenticator returns "Unable to sign request, Unable to find a unique name".
<b>741332</b>	FortiToken email activation sent to user again when LDAP sync runs after the timeout of token activation (user should stay disabled).
<b>744916</b>	Sort by name the sponsor list in the self-registration guest portal.
<b>737727</b>	Change in the password complexity rule is not taking effect.
<b>737078</b>	Private IPv6 address added to SSO list instead of public IPv6 when received from a RADIUS accounting source.
<b>706998</b>	GUI crashes during password recovery using E-mail address method if the E-mail is not associated with any user account.
<b>694599</b>	Certificate sync does not work from Master to LB Peer/Nodes.
<b>760580</b>	Deleting an unused group gives "500 internal server error".
<b>723065</b>	HA connection status is still showing connected even the Primary FortiAuthenticator is already shutdown.
<b>747259</b>	FSAE is taking high CPU.
<b>711940</b>	Raid widget is showing wrong status.
<b>685295</b>	Implement correct handling of VM license in case of configuration conversion.
<b>733788</b>	FortiAuthenticator Agent does not support UPN username format (as imported to the FortiAuthenticator).
<b>721189</b>	SMS : No update on number of sent message on the dashboard.
<b>738349</b>	SAML querying the LDAP when the user is admin instead of looking for the user locally on remote LDAP users.
<b>709395</b>	High CPU utilization by wmid process.
<b>711721</b>	Groups sorting differences when importing LDAP groups in SSO groups and FortiGate filtering.
<b>756786</b>	Guest portal authentication request failed with Cisco WLC.
<b>754474</b>	SAML- SP Login page does not present the Done button in OSX CNA.
<b>586851</b>	http of the FortiAuthenticator cannot be closed.
<b>752572</b>	Windows machine login caching not working and breaking user + machine authentication RADIUS policy condition.
<b>752954</b>	SAML SP ACS URL misconfig returns a Server 500 vs 403 and the log for SP config mismatch.
<b>751445</b>	Saving LDAP server config produces: Please submit 0 or fewer forms.

Bug ID	Description
<b>748487</b>	FortiAuthenticator SAML SP requires at least 1 attribute in received SAML assertions from the remote IdP.
<b>731175</b>	Provide skeleton language pack.
<b>746411</b>	SMTP mail: failed to start session with the "Operation now in progress" error.
<b>632248</b>	Unable to provide publisher details/assign code signing certificate to a Smart Connect profile.
<b>691009</b>	FortiAuthenticator-VM 6.0.4 stops authenticating and GUI freezes until reboot is applied.
<b>748560</b>	FortiAuthenticator active-passive cluster plus load-balancing node does not sync properly.
<b>752114</b>	LDAP group query parsing error.
<b>742715</b>	"The username is in use and this user cannot be made into an administrator" error.
<b>748187</b>	EAP-TLS policy ignores group filter for cert user, cert user can authenticate even if it is not a member of the group.
<b>746538</b>	When applying the OpenLDAP template the out of the box User Object class does not find any user.
<b>742775</b>	Wrong message when user inputs incorrect email address or an incorrect username.
<b>730474</b>	FortiAuthenticator IdP proxy fails to proxy SAML assertions received from remote IdP when the User Attribute with same name exists.
<b>708384</b>	SAML IdP proxy session not showing and unable to log out from an external IdP.
<b>756657</b>	Error while changing HA password of Load Balancer node with HA enabled.
<b>752752</b>	LB + GUI local service certificate restrictions preventing reconfiguration.
<b>731442</b>	Case sensitive remote RADIUS username does not work well.
<b>758407</b>	SP metadata import causes GUI index error.
<b>752730</b>	RADIUS auth fails with invalid user if temporary token type = sms but no mobile number.
<b>756154</b>	Hide self-service portal token registration options when all are disabled.
<b>754134</b>	iOS 14 and iPhone 13 Safari browser: Error displayed on FIDO auto-start after password authentication.
<b>752749</b>	Remote LDAP server page loads incredibly slowly when many imported users exist.
<b>755111</b>	Issue with auto-redirect on HA administration page when enabling HA for load balancer role.
<b>735940</b>	Unable to restart radiusd in debug mode from FortiAuthenticator GUI debug tab after CSP changes for JS.
<b>753040</b>	HA status page should show "Name" of LB nodes in Cluster + LB mode.
<b>752732</b>	Admin trusted hosts applied to SAML auths, not just admin GUI.
<b>742657</b>	Test SMS phone number is not initialized.
<b>748148</b>	ubkey self-provisioning is broken.
<b>733585</b>	No log for policy priority change.

Bug ID	Description
<b>740201</b>	User CSV import does group database check once per record.
<b>746096</b>	Upper case is not accepted for local users.
<b>706422</b>	LB should not delete certificates if they are used by config_setting table but not synced.
<b>744732</b>	FSSO eventlog polling fail for machine account ending with \$.
<b>744505</b>	Unable to see top row title of replacement messages.
<b>739528</b>	Certificate CN validation gives wrong error.
<b>752755</b>	Customized SAML Token Login page's pre-existing pollTokenAuthResult JS broken after upgrade to 6.4.0.
<b>742719</b>	CPU usage 100% after clicking LDAP server in GUI in a customer setup (and GUI timeout).
<b>755701</b>	ESX deploy script.
<b>753032</b>	IdP logins for SP throwing SQL errors on missing session.
<b>753060</b>	User simultaneously created duplicate IdP session - resulted in broken session.
<b>752753</b>	System Access inaccessible if web certificate /CA are missing.
<b>554763</b>	Frequent CSRF errors when using HTTP authentication.
<b>752747</b>	LDAP sync appears to be updating every user record, including unmodified ones.
<b>750732</b>	Login activity not relayed from LB nodes to Master (for user expiry, etc).
<b>740202</b>	Better error-reporting when trying to restore a config which is for a different model.
<b>735652</b>	Unnecessary deletes on load-balancer causes really long re-sync delays.
<b>752242</b>	Logs: FortiAuthenticator should log details when FIDO registration fails.
<b>753921</b>	Change label wording for "Pre-Login Services "==" FIDO Revocation".
<b>752226</b>	FIDO: "Clear all Keys" should delete the keys.
<b>744134</b>	FortiAuthenticator should show "FIDO" in the token column of user page if user has registered a FIDO token.
<b>751543</b>	FTC- user_ip field in auth request is using Country value instead of IP.
<b>744287</b>	OpenSSL 1.1.1l security fixes -- August 2021.
<b>747232</b>	Pillow--- Precaution upgrade.
<b>718365</b>	HA Cluster not able to access management port IP.
<b>739187</b>	REST API authentication for remote user with upper case should not return 401.
<b>758164</b>	Remote RADIUS user case sensitivity is not working properly.
<b>736062</b>	PCI enabled FIDO authentication portal does not work with FIDO user.

Bug ID	Description
<b>737640</b>	Sync rule with multiple OTP assignment methods fails to sync users over if they are missing any one of the LDAP attributes.
<b>745963</b>	Unable to retrieve FIDO token 500 internal server error.
<b>752616</b>	Rephrase label "Every configured password and OTP factors".
<b>576467</b>	Request-URI too long error when we try to export or E-mail large amounts of newly created guest users.
<b>558658</b>	Rephrase timeout error message for timeout in deleting FTC user.
<b>732139</b>	Windows Event Log Sources JavaScript Error.
<b>744577</b>	Cannot import AD user groups as SSO Groups that have '+' in their names.
<b>734462</b>	Extraneous "No search results" message appears under RADIUS Attributes section in user group page.
<b>602248</b>	Migrating a user that already exists causes 500 internal error.
<b>743645</b>	Cannot change the name of local users realm.
<b>739542</b>	Remote RADIUS users with duplicate name REST API call cause 500 errors.
<b>603411</b>	Exporting guest users phone number format incorrect.
<b>736652</b>	New self service portal does not prompt for token resync, allows access with drifted OTP (when within configured window).
<b>734474</b>	LDAP users are able to enable security question through Self-Service portal without actually setting a security question.
<b>732406</b>	Editing security question results in duplicate UI in the pop-up.
<b>731214</b>	500 Internal server error when end user has duplicate certificate bindings.
<b>680974</b>	"Forgot password" option does not work on portal when user is temporary locked.
<b>736020</b>	"None" option for token assignment missing in self-service portal MFA page.
<b>736017</b>	Revoked FIDO token should display time in local time and not UTC.
<b>737638</b>	Missing username in Oauth Request causes 500 server error.
<b>734475</b>	"Internal Server Error" when local user enables security question without setting the security question through captive portal.
<b>579174</b>	FortiToken mobile for a remote radius user on the FortiAuthenticator server and also on the FortiAuthenticator client fails to work.
<b>712166</b>	SCEP gives wrong validation message if "Renewal Days" expiry is left empty.
<b>739570</b>	Unable to create RADIUS attribute matching when creating a RADIUS policy.
<b>734034</b>	Cannot see MAC devices limit in portals settings for Firefox.
<b>734892</b>	FIDO popup message when saving user local information.
<b>758463</b>	FIDO key registration failing first try on iOS 15.1.



Bug ID	Description
<b>761747</b>	Force password change not working when FIDO is enabled in portal policy.
<b>751208</b>	FortiAuthenticator cannot support "mschapv2" as password encoding format for the RADIUS client.
<b>736670</b>	api/v1/ssoauth/ API request returns 500 internal error occasionally.
<b>749559</b>	Windows AD computer authentication option missing from RADIUS policies.
<b>743629</b>	Remote RADIUS user takes longer than 30 sec to verify the deny process.
<b>744073</b>	FortiGate fails to get FSSO list from FortiAuthenticator if the login user group belongs to OU with special characters like +EU.
<b>701758</b>	Problem setting static IP address on a FortiAuthenticator-VM installed on a XenServer.
<b>761875</b>	In the captive portal, when a wrong token code is entered, FortiAuthenticator does not display any error message and just redirects to the login page.
<b>763503</b>	Remote user sync rule does not work with email/FTC 2FA.
<b>762263</b>	PCI mode's behaviour for user without FIDO enabled is incorrect.
<b>762268</b>	Password change not working for remote LDAP users.
<b>603510</b>	Memory usage is High.
<b>763803</b>	LB sync is broken for MAC devices if it is associated to a non-synced user.
<b>746715</b>	Optimize introduction of Load Balancing node(s) to an A-A Cluster to provide high availability.
<b>760305</b>	CLI's "exec ha-rebuild" does not work; cannot find required binaries in PATH.

## Known issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please visit the [Fortinet Support](#) website.

Bug ID	Description
<b>764250</b>	Bug in self-registration of tokens and SMS registration cannot be disabled, although the option is available.
<b>764256</b>	FSSO - LDAP user/group lookup is broken by addition of remote LDAP for computer-based authentication.
<b>763568</b>	The timestamp of the account status for lockout is Greenwich Mean Time 00:00 regardless of system time.
<b>752627</b>	Token transfer fails if includes deprovisioned token(registration id = null) and FortiAuthenticator throws an unknown error.
<b>759691</b>	FSSO self-service portal does not create FSSO session upon end user login.
<b>706701</b>	FortiAuthenticator cluster is inconsistently accessible via HA interfaces from outside the HA subnet.
<b>746567</b>	Importing Local Users from CSV - FortiAuthenticator LB shows 'In Sync with Anomalies'.
<b>745497</b>	Kerberos not working for AES.
<b>676985</b>	Cannot import all FTK hardware tokens from the same purchase order; need to add them all manually.
<b>665384</b>	HA failover does not work reliably after maintenance mode is disabled on the high priority node.
<b>754943</b>	FortiAuthenticator users certs marked as revoked even after expiry date. Deleting is prohibited for some and it produces browser's console errors.
<b>756782</b>	FortiAuthenticator GUI cannot show how many users on every group.
<b>758516</b>	FortiAuthenticator HA: cluster out of sync if custom RADIUS dictionary is uploaded; auth breaks.
<b>757968</b>	/api/v1/pushauth/: the processing of the response is delayed.
<b>764147</b>	Cloud-init: DHCP client stays resident rather than exiting after boot as intended.
<b>764092</b>	Oauth setting permissions are missing.
<b>763026</b>	No popup error if HA table mismatched.
<b>746405</b>	LB HA primary locked SQL database around the same time the disk load-balancer became full.
<b>761702</b>	Unable to properly config postgres for memory/cache if config backup is used.
<b>764179</b>	Unable to change password of remote user unless imported in FortiAuthenticator.
<b>762262</b>	Password reset does not work for remote LDAP user if the password contains 6 characters or less.
<b>763341</b>	Dump when adding LDAP uid to a uid.
<b>690126</b>	HA cluster with load balancer initial setup causes secondary cluster member to crash.

Bug ID	Description
<b>506112</b>	This post REST API call fails to activate the FortiGuard messaging license.
<b>613164</b>	Google Workspace open LDAP crashes when we try to change password.
<b>761880</b>	Trying to get OAuth authorization code for a user with a cloud FortiToken causes django to crash.
<b>761482</b>	FIDO2 authentication not compatible with Apple's WiFi popup.
<b>755752</b>	Power supplies show voltage input fault on both CLI and GUI.
<b>763997</b>	Token challenge not sent to remote RADIUS server when TACACS+ is used with LDAP realm+ chained token.
<b>751108</b>	FortiAuthenticator does not support admin OIDs from FORTINET-CORE-MIB properly.
<b>762203</b>	FSSO Server restart takes too long when global pre-filter gets modified.
<b>761292</b>	Azure remote IdP authentication fails if FortiAuthenticator FQDN contains upper case.
<b>676532</b>	When FortiAuthenticator has a RADIUS client set as subnet; RADIUS accounting disconnect messages are not sent.
<b>758008</b>	FortiAuthenticator joining domain and using the incorrect domain name (DNS) if the name is the same in several LDAP servers.
<b>749422</b>	REST API script is unable to modify user's info when yubikey is assigned.
<b>757460</b>	Enable Django auto-translation for any end-user pages.
<b>756777</b>	Incorrect order of the fields displayed on change_password_remote page for remote users.
<b>566145</b>	Usage Profile "TIME USAGE=Time used" is not triggering COA or a disconnect request to FortiGate.
<b>750134</b>	FortiAuthenticator as LDAP server cannot export admin users from local user base.
<b>748862</b>	Read-only admin profile cannot view local/remote users; error 500.
<b>655350</b>	The lockout policy does not appear to apply to username/token submissions to the /auth API endpoint.
<b>646299</b>	Nutanix AHV KVM based Hypervisor- upgrading FortiAuthenticator from 6.0.4 to 6.1.x fails and hangs on "Waiting for Database".
<b>643810</b>	CLI restore-admin command needs improvement.
<b>638374</b>	SCEP - Encryption/hash compatibility with clients.
<b>637028</b>	SSL connection failed when the certificate expired issue is not explicit enough.
<b>745433</b>	CLI 'execute backup config ftp' upload problem when a path is provided.
<b>677932</b>	SCEP returns 200 on bad requests.
<b>745419</b>	CLI 'execute backup config tftp' (also ftp) with encryption password does not result in encrypted backup.
<b>620127</b>	Changing from maint-mode-no-sync to maint-mode-sync does not appear to restore syncing.
<b>757516</b>	Local user CSV export does not handle commas.
<b>646764</b>	CLI "get disk *" command fails on KVM.

Bug ID	Description
<b>506543</b>	500k+ users- Secondary's SNMP SQL query to obtain user count is obnoxiously slow (postgres needs vacuum full).
<b>742722</b>	Remove SSO on legacy self-service portal.
<b>752408</b>	Seek confirmation from FortiAuthenticator admin when restoring configuration via GUI.
<b>752409</b>	Redirect FortiAuthenticator to a new IP when admin changes the IP through which s/he is accessing it in a browser.
<b>516357</b>	LB - Toggling LB off and back on in an existing cluster can impact availability for hours/days.
<b>586813</b>	Send SNMP trap when active HA master detects that passive unit stopped syncing.
<b>725800</b>	IAM username validation not consistent in REST API.
<b>733323</b>	PCI DSS 2FA shows different page for user that does not exist.
<b>733028</b>	404 Not Found when we Resend email or SMS Message.
<b>723677</b>	Failed auth after changing port on secure LDAP server locks radiusd and prevents it from being killed.
<b>561506</b>	RADIUS auths fail if no port on FortiAuthenticator is assigned an IPv4 address.
<b>674164</b>	Logging into the CLI with incorrect password on the HA secondary gives bunch of SQL errors.
<b>689458</b>	HA cluster changing secret on primary to match secondary causes the webserver to crash on the secondary.
<b>550802</b>	Data persistence for authentication activity widget.
<b>763973</b>	Sponsor admin profile should be read-only.
<b>746611</b>	RADIUS authentication delay causes 2FA failure.

## Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.



The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model						
		200E	300F	400E	800F	1000D	2000E	3000E
<b>System</b>								
Network	Static Routes	50	50	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20	20	20
	SMS Gateways	20	20	20	20	20	20	20
Administration	SNMP Hosts	20	20	20	20	20	20	20
	Syslog Servers	20	20	20	20	20	20	20
	User Uploaded Images	40	90	115	415	515	1015	2015
	Language Files	50	50	50	50	50	50	50
<b>Realms</b>		20	60	80	320	400	800	1600
<b>Authentication</b>								
General	Auth Clients (NAS)	166	500	666	2666	3333	6666	13333

Feature		Model						
		200E	300F	400E	800F	1000D	2000E	3000E
	<b>Users</b> (Local + Remote) <sup>1</sup>	500	1500	2000	8000	10000	20000	40000
	User RADIUS Attributes	1500	4500	6000	24000	30000	60000	120000
	User Groups	50	150	200	800	1000	2000	4000
	Group RADIUS Attributes	150	450	150	2400	600	6000	12000
	FortiTokens	1000	3000	4000	16000	20000	40000	80000
	FortiToken Mobile Licenses <sup>2</sup>	200	200	200	200	200	200	200
	LDAP Entries	1000	3000	4000	16000	20000	40000	80000
	Device (MAC-based Auth.)	2500	7500	10000	40000	50000	100000	200000
	RADIUS Client Profiles	500	1500	2000	8000	10000	20000	40000
	Remote LDAP Servers	20	60	80	320	400	800	1600
	Remote LDAP Users Sync Rule	50	150	200	800	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	4500	6000	24000	30000	60000	120000
	<b>FSSO &amp; Dynamic Policies</b>							

Feature		Model						
		200E	300F	400E	800F	1000D	2000E	3000E
FSSO	FSSO Users	500	1500	2000	8000	10000	20000	200000 <sup>3</sup>
	FSSO Groups	250	750	1000	4000	5000	10000	20000
	Domain Controllers	10	15	20	80	100	200	400
	RADIUS Accounting SSO Clients	166	500	666	2666	3333	6666	13333
	FortiGate Services	50	150	200	800	1000	2000	4000
	FortiGate Group Filtering	250	750	1000	4000	5000	10000	20000
	FSSO Tier Nodes	5	15	20	80	100	200	400
	IP Filtering Rules	250	750	1000	4000	5000	10000	20000
Accounting Proxy	Sources	500	1500	2000	8000	10000	20000	40000
	Destinations	25	75	100	400	500	1000	2000
	Rulesets	25	75	100	400	500	1000	2000
<b>Certificates</b>								
User Certificates	User Certificates	2500	7500	10000	40000	50000	100000	200000
	Server Certificates	50	150	200	800	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	10	50	50	50	50
	Trusted CA Certificates	200	200	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200	200	200
SCEP	Enrollment Requests	2500	7500	10000	40000	50000	100000	200000

<sup>1</sup> Users includes both local and remote users.

<sup>2</sup> **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

<sup>3</sup> For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.



## Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.



The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of auth clients (RADIUS and TACACS+) that can authenticate to the system is:

$$100 / 3 = 33$$

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "-". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
<b>System</b>					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19 (minimum)	250
	Language Files	5	50	50	50
<b>Authentication</b>					
General	Auth Clients (RADIUS and TACACS+)	3	Users / 3	33	1666

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
User Management	Authentication Policy (RADIUS and TACACS+)	6	Users	100	5000
	<b>Users</b> (Local + Remote) <sup>1</sup>	5	*****	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) <sup>2</sup>	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
<b>FSSO &amp; Dynamic Policies</b>					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users / 100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
	FSSO Filtering Object	30	Users x 2	200	10000
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
<b>Certificates</b>					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	500	25000

<sup>1</sup> Users includes both local and remote users.

<sup>2</sup> **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.